Service Acceptable Use Policy

December 2022 v1

1.0 Introduction

This document is copyright TIEVA Ltd and is for internal use and customer information.

The purpose of this document is to define the Service Description provided within the Services (the "Service") from TIEVA Ltd (the "Company") to the Customer ("Customer") under the Service Contract, which is the contract document defining Customer requirement from the Service. The Service is designed to be available, secure, fast, resilient, and scalable accommodating current and future requirements of the Customer within contract parameters.

This document should be read in conjunction with all associated documents: Service Acceptable Use Policy, Service Description, Service Level Agreement (SLA), Service Contract, which specifies prices, and the Terms and Conditions of Service, all of which govern the Service.

The Service includes modular solutions, which can be selected individually or in combination according to Customer requirement and preference. The SLA covers the Service commitments by the Company underpinning all Services, including general IT support of the Customer's technology.

2.0 Cloud Services

Cloud Services are provided on datacentre platform technologies, including private cloud, public cloud (hyperscale), hybrid cloud, and/or on-premise.

3.0 Policy

The Customer is responsible for any violations of this AUP by anyone using the Service, whether authorised or not.

Any queries regarding this AUP must be addressed to the Company Service Director. The Company reserves the right to withdraw and/or suspend the Service immediately should breach of any of the following occur:

3.1 Internet Abuse

The Internet provision within the Service must NOT be used for:

- Attempted or actual unauthorised access to data, services, systems or networks, including probe, scan, test, or breach security or authentication measures without the express permission of the owner of the system or network ("hacking");
- Attempted or actual interference with Service to any host or network including, without limitation, "mailbombing", "flooding", deliberate attempts to overload a system and broadcast attacks;
- Attempted or actual use of an Internet account or computer without the owner's permission;
- Attempted or actual collecting of information by deceit, including, but not limited to "Internet scamming", "password robbery", "phishing" and "port scanning";
- Use of any false, misleading, or deceptive TCP-IP packet header or any part of the header information in an Internet posting;
- Use to distribute software that covertly gathers information about a user or covertly transmits information about the user;
- Any activity that is likely to result in retaliation against the Service;

- Any activity related to downloading or transmitting copyrighted materials including text, music, software, art, images, or other material for which the Customer has no license or does not have the express permission of the copyright owner;
- Any activity or conduct that is likely to be in breach of any applicable laws, codes, or regulations, including Data Protection;
- Introducing intentionally or knowingly into the Service any virus or other contaminating program or fail to use an up to date virus-scanning program on all material downloaded from the Service;
- Any activity or conduct that unreasonably interferes with the use of the Service.

3.2 Email Abuse

The email provision within the Service must not be used for:

- Unsolicited bulk email contravening the European Directive 2002/58/CE of 12 July 2002 on Privacy and Electronic Communications, which states that the use of email for direct marketing is only allowed to recipients who have given their prior consent other than for market research purposes;
- Sending or relaying of unsolicited email ("spam");
- Continued issue of unsolicited email to any person who has indicated that they do not wish to receive it ("opt-out");
- Obscuring the source of email in any manner. Email must include the senders or recipients e-mail address in the body of the message or in the 'TO' line of the email;
- Use of any false, misleading, or deceptive header or part of the header information in an email;
- Use of third party email services that do not have similar procedures covering the above points;

3.3 Offensive Content

The Service must not be used to publish, display, or transmit any materials or content that the Company reasonably believes:

- Constitutes or contains imagery, text, or links related to child pornography or "grooming" (this will be immediately notified to the Police);
- Constitutes or contains imagery, text, or links related to pornography or is otherwise obscene or sexually explicit;
- Constitutes or contains imagery, text or links related to violence, incitement to violence, threats, or can be construed as harassment;
- Includes reference to any activity or conduct that is or may be defamatory, pornographic, obscene, indecent, abusive, offensive, or menacing;
- Is defamatory or violates a person's privacy;
- Is discriminatory of age, race, religion, sex, or sexual orientation;
- Is deceptive under the consumer protection laws, including chain letters and pyramid schemes;
- Creates a risk to a person's safety or health or a risk to public safety or health;
- Compromises national security or interferes with an investigation by law enforcement bodies;
- Infringes another person's trade or service mark, patent, technical copyright, or other property right;
- Involves theft, fraud, drug-trafficking, money laundering or terrorism or is otherwise illegal or solicits illegal conduct;
- Is otherwise malicious, fraudulent, or may result in offence or legal action.

3.4 Security

The Company recommends that Customers operate an internal Service/System Acceptable Use Policy for all staff and contractors with a written/signed policy being held on personnel file and breach of such policy being a disciplinary offence. The Policy should contain provision and acceptance of automated monitoring of communications and systems and definition of Acceptable Use of the system specific to the requirements of the Customer and protecting the Customer's business needs and vicarious liabilities.

The Service must be used by the Customer observing reasonable security measures including:

- All Service user accounts should be individual and non-generic;
- Service usernames and passwords must not be shared or disclosed;
- Passwords should be reasonably complex (8-character minimum containing alpha and numeric characters with case variations;
- Passwords should be changed on a regular/cyclical basis;
- Physical access to network Service equipment (routers, switches, etc) must be secured by means of a locked cabinet and/or room;
- Copies of all Software licenses, discs, agreements, Hardware serial numbers, and local data on-site should be securely stored off-site.

3.5 Legal Compliance

The Company may monitor any content or traffic belonging to the Customer or the Customer's Service Users to ensure the Service is used lawfully. The Company may intercept or block any content or traffic belonging to the Customer where the Service is being used unlawfully or not in accordance with this AUP. Such interception or block will be notified to the Customer by the Company. The Company is, however, under no duty to monitor or govern Customer data and/or activities, and the Company disclaims any responsibility for any misuse of the Service by the Customer or its agents or staff.

In accordance with UK and International law, the Company is legally obliged to suspend the Service and/or provide data to recognised authorities such as the Police and/or HM Customs & Excise on demand.

3.6 IP Addressing

The Customer must only use IP addresses assigned by the Company and not take any action or inaction, which directly or indirectly results in any the Company IP space being listed on any abuse database.

3.7 Software

The Customer must not remove, copy, modify or obscure any copyright trademark or other proprietary rights notices contained in or on the Software provided. While the Company is an approved licensor of specific software, all Software remains the intellectual property of the respective Software authors.

The Company and the respective Software authors disclaim, to the extent permitted by applicable law, all liabilities for any damages, whether direct, indirect, or consequential arising from the Software and or its use. The Customer must not attempt to copy, distribute, reverse engineer, decompile, or otherwise disassemble any of the Software provided, except to the extent that such activity is permitted by applicable law.

Software technical support to the Customer is managed by the Company in conjunction with respective Software authors. With the exception of the Customer's own or proprietary Software (for which the Customer must make their own arrangements), the Company has agreements in place to escalate support to the Software authors should this be required.

The Company has an obligation to regularly disclose Customer information and Software usage information to the Software authors within the bounds of Data Protection legislation, and the Customer agrees to such disclosure.

'No High-Risk Use' – Software is neither designed nor intended for use in a situation where Software failure could lead to death or serious bodily injury of any person, or to severe physical or environmental damage. High-Risk Use includes but is not limited to the following examples: aircraft or other forms of mass human transportation, nuclear or chemical facilities and or medical devices.

The Customer shall indemnify the Company from all liability, including without limitation legal expenses, arising out of; any act or omission on the Customers part; any claims where the use or operation of Customer Software infringes the intellectual property rights of a third party; any fault in Customer Software, provided that the Company provide written notice of such claims, permits the Customer to defend or settle such claims and provide all reasonable assistance to the Customer at the Customers expense.

3.8 Illegal Activities

The Company will, without notice to the Customer, report to the appropriate authorities any action or conduct that it believes is illegal.

4.0 Serious breaches of this AUP

The Company reserves the right to immediately withdraw and/or suspend the Service should a serious breach of this AUP occur, one which may involve illegal activity or suspected illegal activity. This may result in immediate suspension of the Service, termination of the Service and/or referral to the Authorities.

5.0 Other Breaches

Other breaches will be notified by the Company to the Customer as a formal written notice of the breach. Should the Customer not rectify the breach and confirm written notice of such rectification within 30 days from the Company's notice of breach, the Company may consider the Customer to be in of the Service Contract, which may result in a suspension or termination of the Service.